METHODS AND SYSTEMS FOR ANALYZING SECURITY EVENTS

Abstract of the Invention

In one aspect, the technology relates to a method for analyzing a security event in a distributed fashion. The method includes the steps of detecting an occurrence of a security event within a customer network and querying a first component of the customer network for data in response to the detected occurrence of the security event. The method also includes the steps of receiving, by a data monitor located within the customer network, first data from the component in response to the query and determining, based on the received first data, whether to query for additional data. The method additionally includes querying at least one of the first component and another component of the customer network to obtain the additional data in response to the determining step, and analyzing the security event using at least one of the first data and the additional data.